

WAYS TO PROTECT AGAINST IDENTITY THEFT AND IDENTITY (ACCOUNT) FRAUD:

Identity theft and fraud refer to crimes where a person wrongfully obtains and uses another person's personal data (e.g., credit card, social security number) that involves fraud or deception usually for economic gain. The government estimates that there are over 400,000 people victimized by these crimes each year. Below are some easy steps you can take to minimize the chances that you will be included in this statistic.

- **Protect your personal data.** Always be conscious of someone that may be "*shoulder surfing*" or listening as you punch in your credit card pin number, telephone calling card number or give out a credit card number over the phone.
- Never give out financial information over the phone unless you placed the call or know the person or organization with whom you are dealing. **Adopt a need to know.** Especially beware of a person that calls you on the phone with offers for valuable items in return for personal data. This is also true for unsolicited e-mail, or SPAM, that requests financial or personal information in return for some benefit.
- Be careful of the information that you have printed on your checks or that appears on your driver's license. You don't need your SSN on your checks and don't use your SSN as your drivers license number unless required by your State.
- Copy important contents of your wallet on a photocopy machine, do both sides of each license, credit card, etc. You will know what you had in your wallet and all of the account numbers and phone numbers to call and cancel. Keep the photocopy in a safe place. It's also a good idea to carry a photocopy of your passport when traveling abroad.
- Check your financial information regularly. This includes all bank and credit card statements. Know what should be there and what shouldn't be there. Ask periodically for copies of your credit report from one of the three major credit bureaus (listed below).
- Be careful when disposing of important financial documents and financial solicitations. Tear them up or shred them.

What should you do if you become a victim of identity theft?

The most important thing is to act immediately to minimize damage to your personal funds, credit and reputation.

- Notify your credit card companies and bank. The key here is having their toll-free numbers and your card and account numbers handy so you know whom to call.
- Call the three national credit reporting organizations immediately to place a fraud alert on your name and Social Security number. The alert means any company that checks your credit knows your information was stolen and they have to contact you by phone to authorize new credit. The numbers are:

Equifax: (800) 525-6285

Experian (formerly TRW): (888) 397-3742

Trans Union: (800) 680-7289

- Contact the [Social Security Administration](#) online or call its fraud line at (800) 269-0271 if you suspect your SSN is being fraudulently used.
- If your wallet is stolen file a police report immediately. This proves to credit providers you were diligent and is a first step toward an investigation.
- You can also file a complaint to the [Federal Trade Commission](#) online or by phone at (877) 438-4338. FTC serves as the federal clearinghouse for complaints by victims of identity theft. While the FTC does not resolve individual consumer problems, your complaint helps them investigate fraud, and can lead to law enforcement action.